



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/808,973	03/24/2004	Ned M. Smith	42P18125	7029
45209	7590	08/25/2008	EXAMINER	
INTEL/BSTZ			TRAORE, FATOUUMATA	
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP			ART UNIT	PAPER NUMBER
1279 OAKMEAD PARKWAY				2136
SUNNYVALE, CA 94085-4040				
			MAIL DATE	DELIVERY MODE
			08/25/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/808,973	SMITH, NED M.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 17 June 2008.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-5, 10, 11, 13-15, 33-37, 42, 43 and 45-47 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-5, 10-11, 13-15, 33-37, 42-43, 45-4 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____ .
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)	5) <input type="checkbox"/> Notice of Informal Patent Application
Paper No(s)/Mail Date _____.	6) <input type="checkbox"/> Other: _____ .

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on June 17, 2008 has been entered. Claims 1-3 and 33-35 have been amended. Claims 16-32 have been withdrawn. Claims 6-9, 12, 33-41 and 44 have been cancelled. Claims 1-5, 7-11, 13-15, 33-37, 42-43 and 45-47 have been amended and have been considered below.

Specification

2. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. In the previous Office Action, claims 33-47 were rejected under 35 U.S.C. 101 because the subject matter is directed to non-statutory subject matter. The 101 rejection to claims 38-41 have been withdrawn in light of the amendment to claims 39-

Art Unit: 2136

41, thus claims 33-37 and 42-43 are still rejected under 35 U.S.C. 101. Applicant's representative argued, "*Applicants' claims are directed to "An article comprising: a tangible storage medium having a plurality of machine accessible instructions stored thereon, wherein when the instructions are executed" Applicants respectfully request clarification as to how the Office can possibly interpret such claim language as "an electronic signal". It is irrelevant what is stated in paragraph [0105] if the claim does not read on a form of energy, which it does not.*"

The examiner asserts that in view of the specification, the limitation of the claims does not fall within the statutory classes listed in 35 USC 101. The language of the claims raises a question as to Whether the claims are directed merely to a abstract idea/storage medium which could be a signal that is not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101

Claims 33-37 and 42-43 recites ***an article comprising: a tangible storage medium having a plurality of machine accessible instructions stored thereon, wherein when the instructions are executed by a processor, the instructions provide for simultaneously authenticating multiple facets of an endpoint.. On applicant's disclosure, on page 34, line 22 to page 35, line 4 or on paragraph [0105] of the disclosure the following has been recited. "The terms "machine readable medium" and "machine accessible medium" shall accordingly include, but not be limited to, solid-state memories, optical and magnetic disks, and a carrier wave that***

encodes a data signal." Such storage medium/machine-readable medium is considered non- statutory. Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1 and 33 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The claims recite the limitation of "*mixing, via a hash algorithm to generate a master secret, the cryptographic hash of the platform configuration with a pre-master secret and data from a stored measurement log that stores configuration state measured values for the endpoint platform .*" However, it is unclear to the examiner where to find support in the specification for the newly amended limitations ***especially generating the master key by hashing which includes the data from a stored measurement log (configuration data or SML).*** Appropriate correction is required.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-5, 10-11, 13, 15, 33-37, 42-43, 45 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Uusitalo et al(US 2005/0063544) in view of Wiseman et al (US 7,216,369).

Claims 1 and 33: Uusitalo et al discloses a security protocol method and an article comprising:

- i. Cryptographically hashing a platform configuration value from a platform configuration register (PCR) in a trusted platform module (TPM) that indicates integrity of an endpoint platform, the platform configuration value representing a configuration state of the endpoint platform that indicates an integrity of the endpoint platform to generate a cryptographic hash of the platform configuration (*for security reasons secret key (k) may not be used directly to encrypt traffic, but rather some traffic encryption key (TEK) is derived from the PMK k (e.g. by taking a hash of the PMK)* (*paragraph [0048]*);
- ii. Negotiating a communication channel(*paragraph [0035]*);
- iii. Signing the master secret with multiple authentication facets of the endpoint, the multiple authentication facets including a user key

representing a particular user and a platform key representing the particular endpoint platform (*in addition to the IMSI it is proposed here that a secret key k is also stored on the SIM card. This key is known only to the network operator and to the user (user key) and a platform form key representing a particular endpoint platform (when a subscriber registers with the operator of a 3GPP network, he or she receives a Subscriber Identity Module (SIM) card on which is stored a unique International Mobile Subscriber Identity (IMSI) code (platform key)(paragraph [0032])*;

iv. Authenticating the negotiated communication channel with the signed master secret to establish the negotiated communication channel as a secure channel to achieve late binding of the secure channel, including generating a session key for the communication channel, where the session key is generated from the master secret (*paragraphs [0048], [0051]*).

However, Uusitalo et al does not explicitly disclose the step of Mixing, via a hash algorithm to generate a master secret, the cryptographic hash of the platform configuration with a pre-master secret and data from a stored measurement log that stores configuration state measured values for the endpoint platform via a hash algorithm to generate a master secret.

Wiseman et al discloses trusted platform , which further discloses a step of Mixing, via a hash algorithm to generate a master secret, the cryptographic hash of the platform configuration with a pre-master secret and data from a stored

measurement log that stores configuration state measured values for the endpoint platform via a hash algorithm to generate a master secret(*column 3, lines 35-45*). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made to include a step of generating a master by hashing a combined value of the platform configuration with a pre-master secret and data from a stored measurement . One would have been motivated to do so in order to provide security for computational platform as taught by Wiseman et al (*column 1, lines 15-20*).

Claims 2 and 34: Uusitalo et al and Wiseman et al disclose a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 1 and 33 above, and Uusitalo et al further discloses that the platform private key is bound to the platform configuration using the TPM (*when a subscriber registers with the operator of a 3GPP network, he or she receives a Subscriber identity Module (SIM) card on which is stored a unique International Mobile Subscriber Identity (IMSI) code (paragraph [0032])*).

Claims 3 and 35: Uusitalo et al and Wiseman et al disclose a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 2 and 34 above, and Uusitalo et al further discloses that the TPM comprises a processor coupled to a protected storage device (*paragraph [0053]; Fig .7*).

Claims 4 and 36: Uusitalo et al and Wiseman et al disclose a method and article of facilitating the lawful interception of an IP session between two or more

terminals as in claims 1 and 33 above, and Uusitalo et al further discloses a step of cryptographically hashing the platform configuration comprises cryptographically hashing the platform configuration using a secure hashing algorithm (*a pseudo-random function such as a keyed hash (or MAC, Message authentication code) such as SHA-1 or MD5 or the 3GPP Milenage algorithm*)*(paragraph [0032]).*

Claims 5 and 37: Uusitalo et al and Wiseman et al disclose a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 4 and 36 above, and Uusitalo et al further discloses that the secure hashing algorithm comprises Secure Hashing Algorithm Version 1.0 (SHA-1) (paragraph [0032]).

Claims 10-11 and 42-43: Uusitalo et al and Wiseman et al disclose a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 1 and 33 above, and Uusitalo et al further discloses wherein the platform configuration includes multiple identities (*Fig. 2*) and the platform key includes one or more platform identity keys*(paragraph [0032]).*

Claims 13 and 45: Uusitalo et al and Wiseman et al disclose a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 1 and 33 above, and Uusitalo et al further discloses that the method and article further comprises:

- v. Exchanging an explanation of the platform configuration hashes following session key negotiations to finalize the authentication (paragraph [0032]);
- vi. Verifying, at both endpoints, key exchange messages, certificates and platform configuration data (paragraphs [0053], [0088]); and
- vii. Authenticating the session if no problems arise during verification (paragraphs [0053], [0054]).

Claims 15 and 47: Uusitalo et al and Wiseman et al disclose a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 13 and 45 above, and Uusitalo et al further discloses a step of enabling endpoints to exchange data, wherein each endpoint knows that the platform from the other endpoint has been authenticated using a platform identity that ties to the trusted platform module (*paragraph [0032]*).

8. Claims 14 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Uusitalo et al (US 2005/0063544)) in view of Wiseman et al (US 7,216,369) in further view of Bass et al (US 4649233).

Claims 14 and 46: Uusitalo et al and Wiseman et al disclose a method and article of facilitating the lawful interception of an IP session between two or more terminals as in claims 13 and 45 above, while neither of them explicitly discloses a step of halting the authentication. However, Bass et al discloses a method and article to support secure data transfer, which further discloses a step of halting

the authentication session if problems arise during verification (column 4, lines 35-51). Therefore, it would have been obvious for one having ordinary skills in the art at the time the invention was made to include a step of halting the authentication. One would have been motivated to do so in order to prevent unauthorized access to critical data.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Monday, August 25, 2008

Application/Control Number: 10/808,973
Art Unit: 2136

Page 11

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136